Listing of Claims:

The following listing of claims will replace all prior versions and listings of claims in the application.

1. (currently amended) A method, implemented with an integrated circuit, for evaluating contents of a message, comprising:

characterizing a message segment, wherein the message segment further comprises a packet in a packet-switched network;

scanning the message segment to define a stream of tokens associated with the message segment;

associating the message segment with a meta session through the stream of tokens, wherein the meta session is made persistent across message transactions and different HTTP sessions by storing data generated by the meta session on a persistent storage medium;

parsing the token[s] stream to extract substructures according to a grammar;

determining rules associated with the tokens, the rules when executed defining actions for intrusion detection and prevention;

executing the actions associated with the message segment; and

queuing the message segment for transmission to a destination.

2. (previously presented) The method of claim 1, further including:

retrieving meta session state information related to the message, wherein the meta session state information is invariant across different connections and a service context common to the different connections associates the different HTTP sessions of a user.

3. (original) The method of claim 1, wherein the message segment is received from a sender, the sender using a network to send a message associated with the message segment, and the message associated with the message segment is identified as a suspect message which is quarantined.

4. (original) The method of claim 1, wherein the method operation of parsing the tokens to extract substructures includes,

creating a parse tree.

5. (original) The method of claim 1, wherein the method operation of determining rules associated with the tokens includes,

defining an object oriented scheme to associate the message segment with at least one of the rules.

6. (original) The method of claim 5, wherein the method operation of defining an object oriented scheme to associate the message segment with at least one of the rules is enabled through grammar based access.

7. (original) The method of claim 1, wherein the method operation of parsing the tokens to extract substructures includes,

searching a list of keywords; and

inferring semantics of sub-strings between the key words.

8. (original) The method of claim 1, wherein the message is composed of multiple segments.

9. (previously presented) The method of claim 8, wherein the substructures span multiple message segments.

10. (currently amended) A computer readable media having computer program instructions for evaluating the contents of a message, comprising

computer program instructions for characterizing a message segment, wherein the message segment further comprises a packet in a packet-switched network;

computer program instructions for scanning the message segment to define a stream of tokens associated with the message segment;

computer program instructions for associating the message segment with a meta session through the stream of tokens, wherein the meta session is made persistent across message transactions and different HTTP sessions by storing data generated by the meta session on a persistent storage medium;

computer program instructions for parsing the token[s] stream to extract substructures according to a grammar;

computer program instructions for determining rules associated with the tokens, the rules defining actions for intrusion detection and prevention;

computer program instructions for executing the actions associated with the message segment; and

computer program instructions for queuing the message segments for transmission.

11. (previously presented) The computer readable media of claim 10, further including:

computer program instructions for retrieving meta session state information related to the message, wherein the meta session state information is invariant across different connections and a service context common to the different connections associates the different HTTP sessions of a user.

12. (currently amended) The computer readable media of claim 10, wherein the computer program instruction for characterizing a message segment includes,

computer program instructions for determining a grammar type of the message.

13. (previously presented) The computer readable media of claim 10, wherein the computer program instructions for parsing the tokens to extract substructures includes,

computer program instructions for creating a parse tree.

14. (original) The computer readable media of claim 10, wherein the message is configured to be sent in multiple segments through a packet based network.

15. (previously presented) The computer readable media of claim 10, wherein the computer program instructions for parsing the tokens to extract substructures includes,

computer program instructions for searching a list of keywords; and

computer program instructions for inferring semantics of sub-strings between the key words.

16. (currently amended) A network device configured to provide content based security, comprising:

circuitry for scanning a message segment to define a stream of tokens associated with the message segment, wherein the message segment further comprises a packet in a packet-switched network;

circuitry for extracting substructures from the stream of tokens, according to a grammar;

circuitry for associating the message with a meta session, wherein the meta session is made persistent across message transactions and different HTTP sessions by storing data generated by the meta session on a persistent storage medium;

circuitry for identifying rules associated with the tokens, wherein the rules define actions for intrusion detection and prevention; and

circuitry for executing the identified rules.

17. cancelled

18. (previously presented) The network device of claim 16, wherein the circuitry for extracting substructures from the tokens includes,

circuitry for retrieving meta session state information related to the message, wherein the meta session state information is invariant across different connections and a service context common to the different connections associates the different HTTP sessions of a user.

19. (original) The network device of claim 16, wherein the circuitry for scanning a message to define tokens associated with the message includes,

circuitry for searching a list of keywords; and

circuitry for inferring semantics of sub-strings between the key words.

20. (original) The network device of claim 16, further comprising:

circuitry for determining a grammar type of the message.

21. (original) The network device of claim 16, wherein the circuitry for scanning a message to define tokens associated with the message includes,

circuitry for building a data structure from the defined tokens.